

Log Message Reference

FortiNDR 7.6.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



November 20, 2026

FortiNDR 7.6.0 Log Message Reference

55-760-1229094-20251120

TABLE OF CONTENTS

Change Log	4
FortiNDR Log Message reference	5
Admin Logins/Logouts	5
Admin/Web Session Authentication	5
System Actions and Setting/Configuration Changes	6
NDR Mute Rule Changes	7

Change Log

Date	Change Description
2025-11-21	Initial release.

FortiNDR Log Message reference

Admin Logins/Logouts

Event	Field Format	Example
Login Success	User <user> login successfully from <GUI(IP)>	User admin login successfully from GUI (203.0.113.45)
Login Failure	User <user> login failed from <SSH (IP)>	User guest login failed from ssh (203.0.113.45)
Logout Success	User <user> logout from <IP address>.	User admin logout from 203.0.113.45.
Logout Timeout	User <user> time out on <IP address>.	User admin time out on 203.0.113.45.
Forced Logout	GUI session forced logout from <IP address>.	GUI session forced logout from 203.0.113.45.
Login Blocked	User <user> login blocked from <SSH (IP)> due to <reason>	User admin login blocked from ssh (203.0.113.45) due to try_too_many_times

Admin/Web Session Authentication

Event	Field Format	Example
Admin Session Failure	Session check failure for user <IP address>	Session check failure for user (203.0.113.45)
Web No Timeout Value	GUI session no timeout value from <IP address>	GUI session no timeout value from (203.0.113.45)
Web Session Timeout	GUI session timeout from <IP address>	GUI session timeout from (203.0.113.45)
Web Failed Check SN	GUI session failed to check SN from <IP address>	GUI session failed to check SN from (203.0.113.45)
Web Failed Start Verify Password	GUI session failed to start verify password from <IP address>	GUI session failed to start verify password from (203.0.113.45)
Web Fail Verify Password	GUI session failed to verify password from <IP address>	GUI session failed to verify password from (203.0.113.45)

System Actions and Setting/Configuration Changes

Event	Field Format	Example
File Upload	file upload request from <IP address>	file upload request from 203.0.113.45
SSH Key Configuration Removed	sshkey configuration removed for user <user (name)> by <user> from <IP address>	sshkey configuration removed for user harry by admin from 203.0.113.45
SSH Key Configuration Added	sshkey configuration added for user <user (name)> by <user> from <GUI (IP)>	sshkey configuration added for user harry by admin from 203.0.113.45
CLI Log Action	<action details> (user: <user>, from: <UI(IP)>)	changed settings of 'ips-dbs' for 'system ndr settings' (user: admin, from: ssh (203.0.113.45))
VM License Updated	VM license has been updated by user <user> via <GUI(IP)> .	VM license has been updated by user admin via GUI(203.0.113.45).
System Configuration Restored	System configuration restored from <source> file (name: <file>, version: <backup version>) on <current version> by user <user> via <UI(IP)>.	System configuration is restored from central management file (name: config.bak, version: v7.6-build0670) on v7.6-build0660 by user admin via 203.0.113.45.
Factory Reset	System has been reset to factory defaults by user <user> via <IP address>.	System has been reset to factory defaults by user admin via ssh(203.0.113.45).
System Upgraded	System firmware has been upgraded from <version> to <version> by user <user> via <IP address>.	System firmware has been upgraded from v7.6-build0001 to v7.6-build0500 by user admin via 203.0.113.45.
System Upgraded (Ver Only)	System <version> has been upgraded by user <user> via <IP address>.	System v7.6-build0660 has been upgraded by user admin via 203.0.113.45.
System Restarted	System <version> has been restarted by user <user> via <SSH (IP)>	**Example: **System (v7.6-build0660) has been restarted by user admin via ssh (203.0.113.45)
System Shutdown	System <version> has been shutdown by user <user> via <SSH (IP)>	System (v7.6-build0660) has been shutdown by user admin via ssh (203.0.113.45)
System Reloaded	System <version> has been	System (v7.6-build0660) has been

Event	Field Format	Example
	reloaded by user <user> via <SSH (IP)>.	reloaded by user admin via ssh (203.0.113.45).
Image Error	Check image error by user <user> via <SSH(IP)>.	Check image error by user admin via ssh (203.0.113.45).
System Configuration Restore Failed	System configuration restoration by user <user> via <IP address> failed.	System configuration restoration by user admin via ssh(203.0.113.45) failed.
System Time Changed	System time changed to <new time> by user <user> via <SSH(IP)>	System time changed to 08/27/2025 15:30:00 by user admin via ssh (203.0.113.45)
License Updated	<license status message>, user=<user>, ui=<UI(IP)>.	management license status changed from 'Expired' to 'Licensed', user=admin, ui=GUI(203.0.113.45).
System DB Restore	System <version> db restored by user <user> via <SSH(IP)>	System (v7.6-build0660) db restored by user admin via ssh(203.0.113.45)

NDR Mute Rule Changes

Event	Field Format	Example
NDR Mute Rule Add	FortiNDR Muting Profile <rule_profile_name> <ID=<rule_profile_id>, Rule ID=<rule_id> add by <user>.	FortiNDR Muting Profile dafesf (ID=99438c56-5150-472b-a406-42633bb1970c, Rule ID=ae134c6e-5241-4fee-8017-882439e27cf6) add by admin.
NDR Mute Rule Update	FortiNDR Muting Profile <rule_profile_name> (ID=<rule_profile_id>, Rule ID=<rule_id>) (created by <user>) modify by <user>.	FortiNDR Muting Profile dafesf (ID=99438c56-5150-472b-a406-42633bb1970c, Rule ID=ae134c6e-5241-4fee-8017-882439e27cf6) (created by dafesf) modify by admin.
NDR Mute Rule Delete	FortiNDR Muting Profile <rule_profile_name> (ID=<rule_profile_id>, Rule ID=<rule_id>) remove by <user>.	FortiNDR Muting Profile dasda (ID=b80c6af8-19c9-4ab4-b339-ccbda017e83a, Rule ID=d4f9ed6f-9515-4965-8566-7041bcd30368) remove by admin.
NDR Mute Rule Delete All	All FortiNDR Muting Profile and Rule remove by <user>.	All FortiNDR Muting Profile and Rule remove by admin.
NDR Mute Rule Delete By Range	FortiNDR Muting Profile and Rule deleted in range <range> by user <user>.	FortiNDR Muting Profile and Rule deleted in range Profile '99438c56-5150-472b-a406-42633bb1970c' by user admin.



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.